Отчет по ДЗ №4

Сетевое взаимодействие

* 1. **Найти номера актуальных RFC для следующих протоколов:**
     1. TCP
     2. UDP
     3. IPv4
     4. IPv6
     5. ICMP
     6. ARP.

Рабочее предложение (англ. Request for Comments, RFC) — документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети. Название «Request for Comments» ещё можно перевести как «заявка (запрос) на отзывы» или «тема для обсуждения». В настоящее время первичной публикацией документов RFC занимается IETF под эгидой открытой организации Общество Интернета (англ. Internet Society, ISOC). Правами на RFC обладает именно Общество Интернета.

|  |  |
| --- | --- |
| **Протокол** | **RFC** |
| TCP | 793 |
| UDP | 768 |
| IPv4 | 791 |
| IPv6 | 2460 |
| ICMP | 792 |
| ARP | 826 |

1. **Ответить на следующие вопросы:**
   1. Что такое IP адрес?

IP-адрес — уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP.

* 1. Что такое маска подсети?

**Маска** **подсети** — битовая **маска** для определения по IP-адресу адреса **подсети** и адреса узла (хоста, компьютера, устройства) этой **подсети**. В отличие от IP-адреса **маска** **подсети** не является частью IP-пакета. Благодаря **маске** можно узнать, какая часть IP-адреса узла **сети** относится к адресу **сети**, а какая — к адресу самого узла в этой **сети**.

* 1. Сколько хостов включает в себя сеть 192.168.1.1/23?

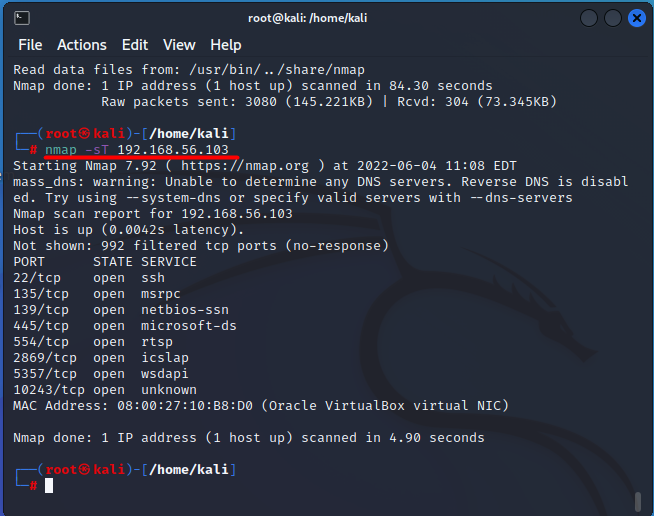
Данная сеть включает в себя 510 хостов.

* 1. Что такое MAC адрес?

МАС адрес (media access control address) – уникальный идентификатор, назначенный сетевому адаптеру, применяется в сетях стандартов IEEE 802, в основном Ethernet, Wi-Fi и Bluetooth.

1. **С виртуальной машины с ОС Kali провести сканирование виртуальной машины следующими типами:**
   * 1. TCP, UDP scan;

TCP-сканирование

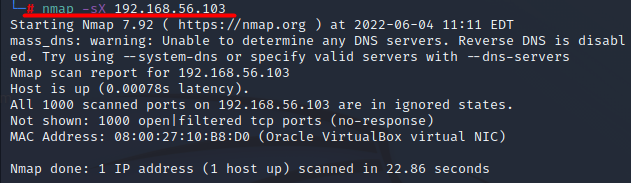


**UDP-сканирование**

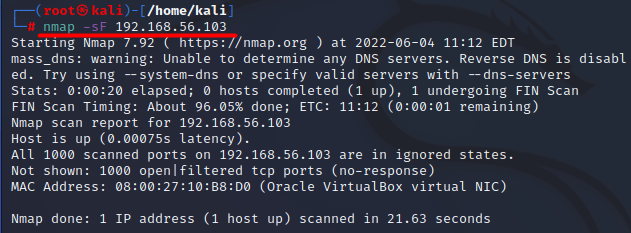


* + 1. Spoofed TCP (То же, что и IDLE);
    2. Xmas, FIN, NULL

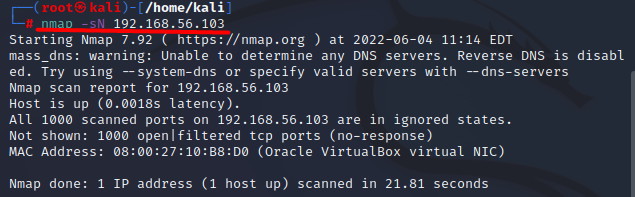
Xmas-сканирование



FIN-сканирование



NULL-сканирование



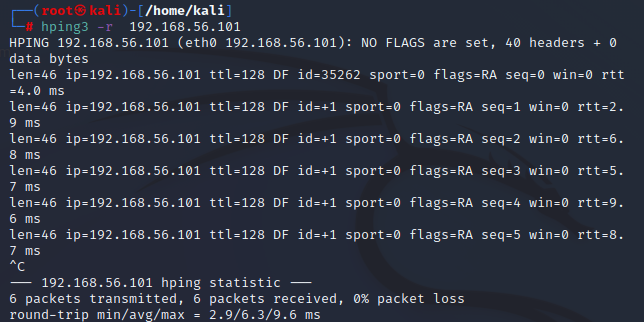
* + 1. **IDLE (в два этапа, сначала поиск подходящей зомби машины, затем сканирование с ее использованием)**

Из списка активных хостов нужно выделить подходящие зомби-хосты. Чтобы удачно их выбрать нужно, чтобы выполнялись два условия[[2]](https://ru.wikipedia.org/wiki/Idle_scan#cite_note-FTech-2):

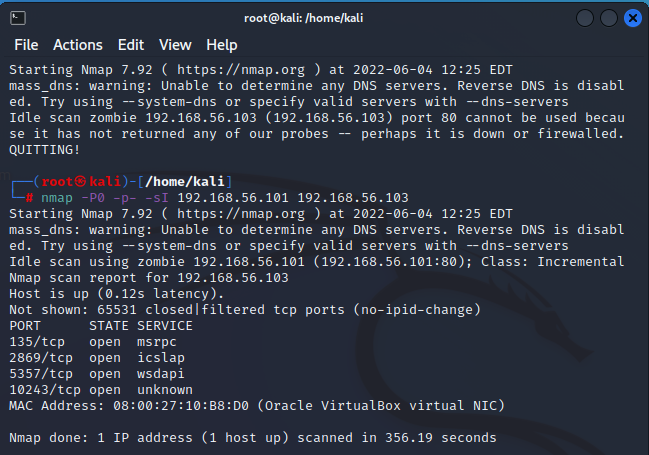
При обмене пакетами с ним его IP ID должен инкрементироваться на единицу

Хост должен быть бездействующим, чтобы посторонний трафик не исказил его IP ID.

Для выполнения задания была поднята виртуальная машина с Windows 10 и отключенным Firewall. Были проверены ID пакетов, таким образом, чтобы ID инкрементировалось на 1.



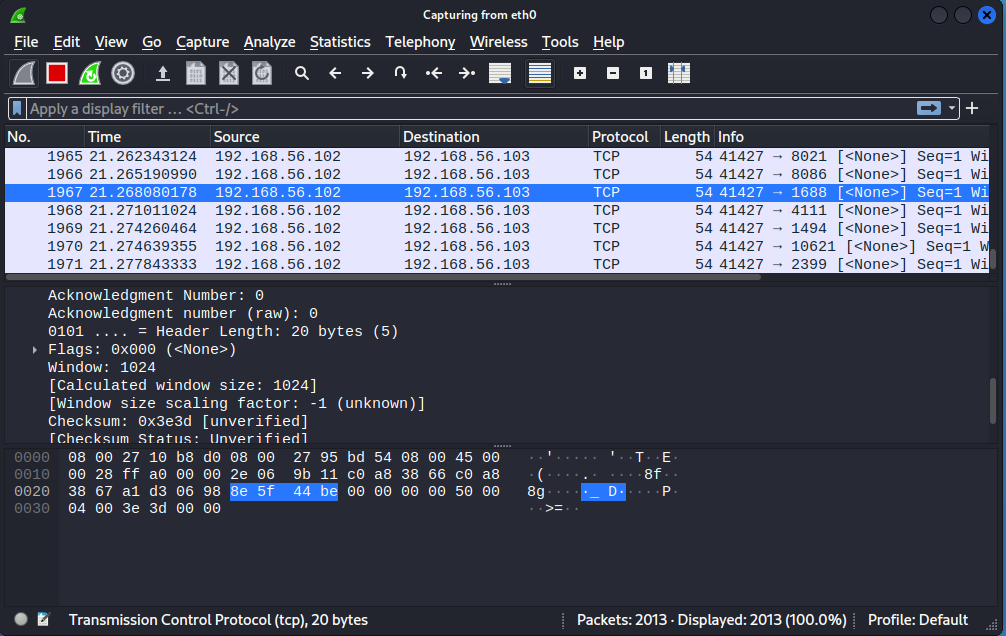
После чего была просканирована целевая машина (Windows 7) с использованием зомби-машины (Windows 10).



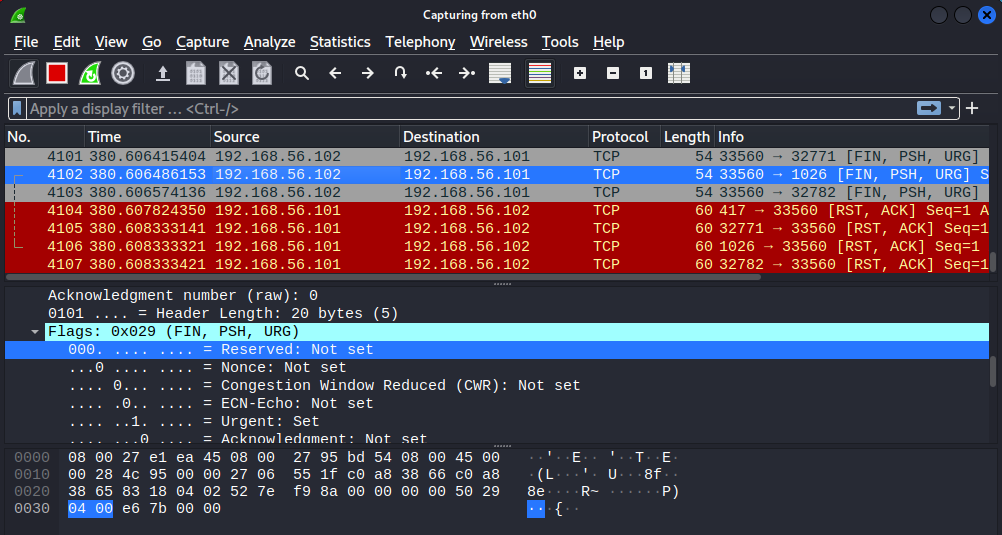
**3.2 Сканирование провести с запущенным Wireshark и затем в логах перехваченных пакетов найти признаки сканирования (SYN пакеты, Xmas пакеты или по адресу цели).**

Методы TCP NULL, FIN, Xmas заключаются в отправке пакетов с отключенными флагами в заголовке TCP. При NULL-сканировании не устанавливаются никакие биты, при FIN-сканировании устанавливается бит TCP FIN, а в Xmas-сканировании устанавливаются флаги FIN, PSH и URG.

Для примера было запущено NULL-сканирование. Из скриншота видно, что ни один флаг не установлен.



При запуске Xmas-сканирования были установлены флаги FIN, PSH и URG.



1. **С виртуальной машины с ОС Kali провести сканирование виртуальных машин в лабораторной сети(или любой другой удобной, возможно домашнего роутера или хостовой машины) с применением скрипта vulners.nse.**

Скрипт определил ОС целевой машины.

